A Balanced Key Management

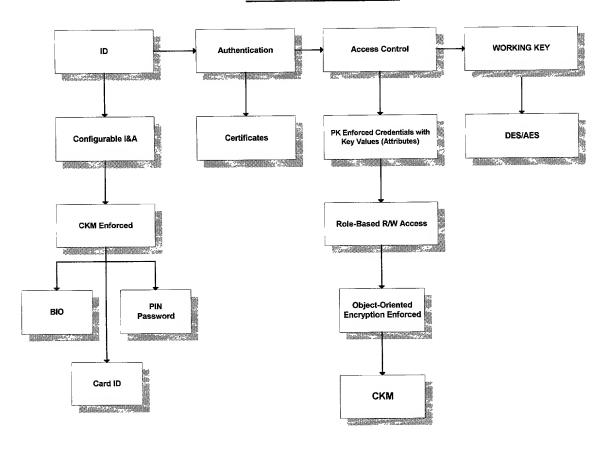


FIG. 1

Smart Token Avenue to Comprehensive Security

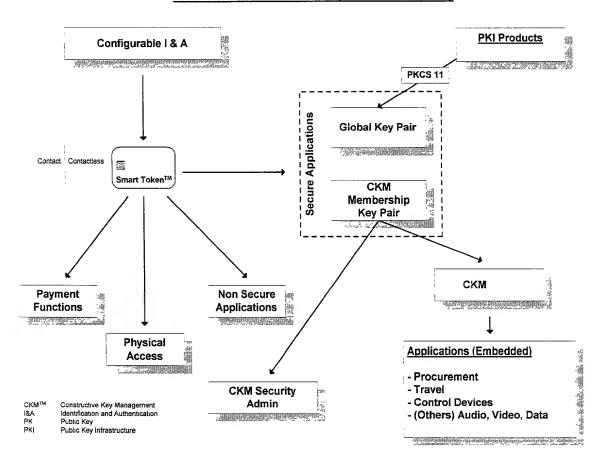


FIG. 2

Diffie-Hellman Random Value Encryption and Decryption

ENCRYPTION

Diffie-Hellman prime modulus

Diffie-Hellman 160-bit prime

generator of group Z_{ρ} number of labels i^{th} derived key

Ephemeral Private Key

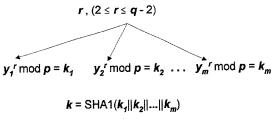
Ephemeral Public Key

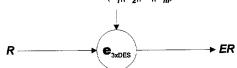
two-key 3xDES key

R Random Value ER Encrypted Random Value

p

q





DECRYPTION

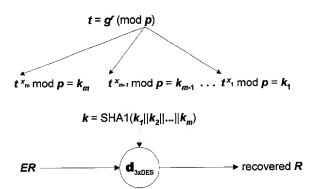


FIG. 3

Combiner Function

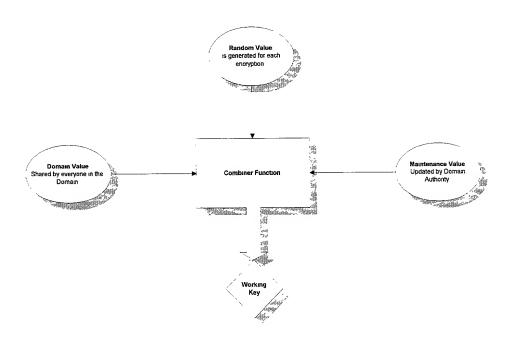
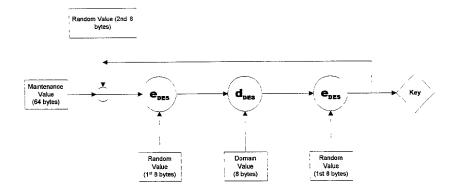


FIG. 4

Combiner Function Using

Triple DES CBC Mode



Legend

e₀ss DES encryption

d₀ss DES decryption
⊕ Exclusive-OR

FIG. 5

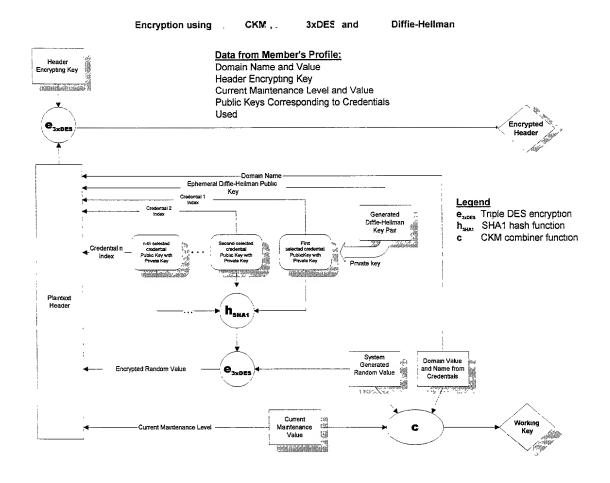
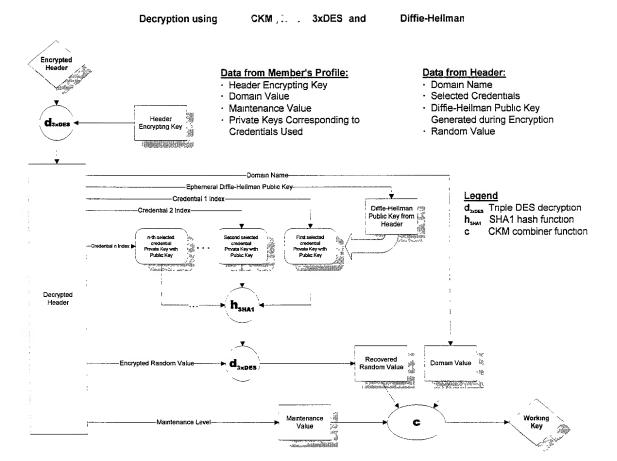


FIG. 6





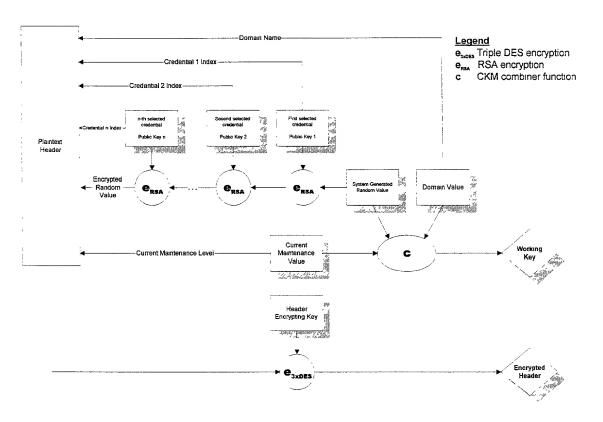


FIG. 8



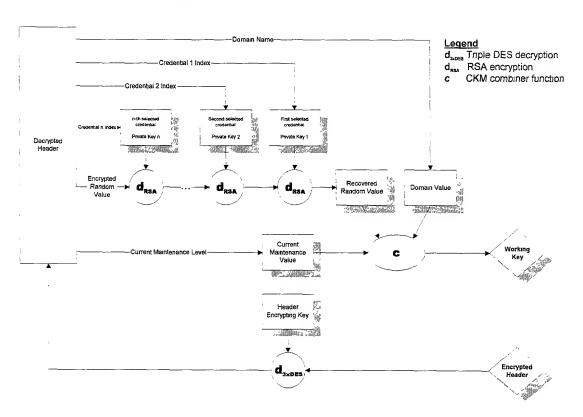


FIG. 9

Maintenance Value and Header Encrypting Key Generation

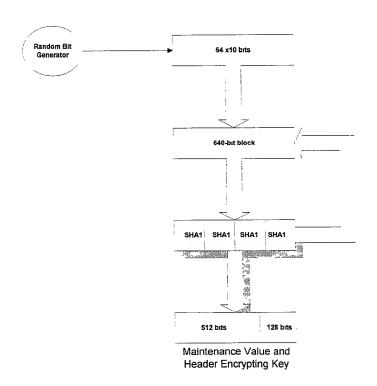


FIG. 11

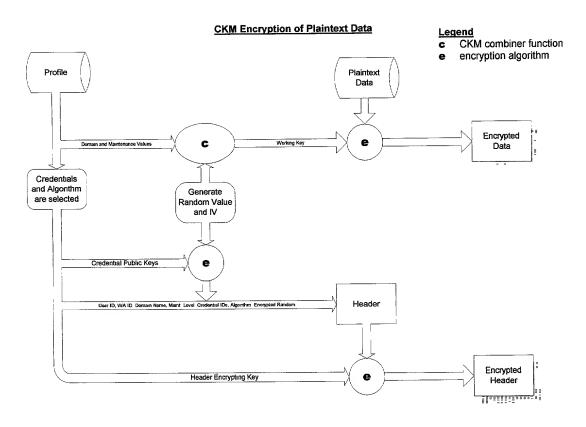
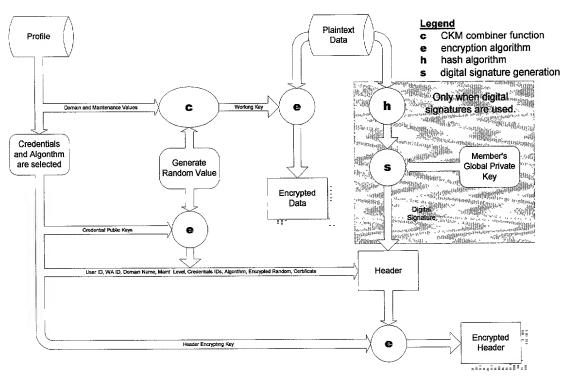


FIG. 12

CKM Encryption with Digital Signature



CKM Decryption Legend c CKM combiner function d decryption algorithm Encrypted Header Encrypted Data Profile Decrypted Data d Encrypted Random Value d Header Key Working Key Credentials found? Credential Ids No Access Yes, continue Credential Private Keys C Maintenance and Domain Values

CKM Decryption with Digital Signature Verification

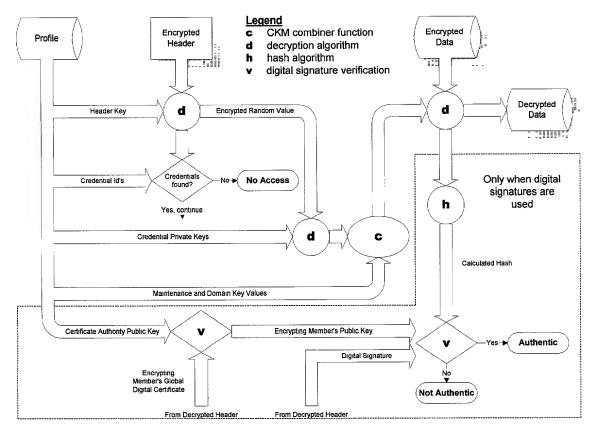


FIG. 14

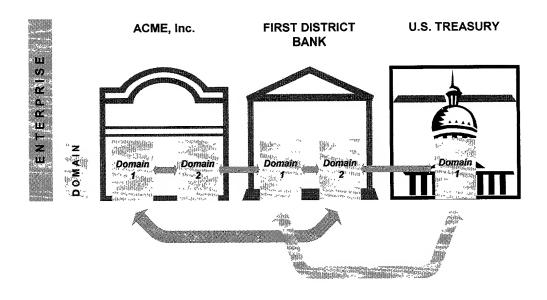


FIG. 15

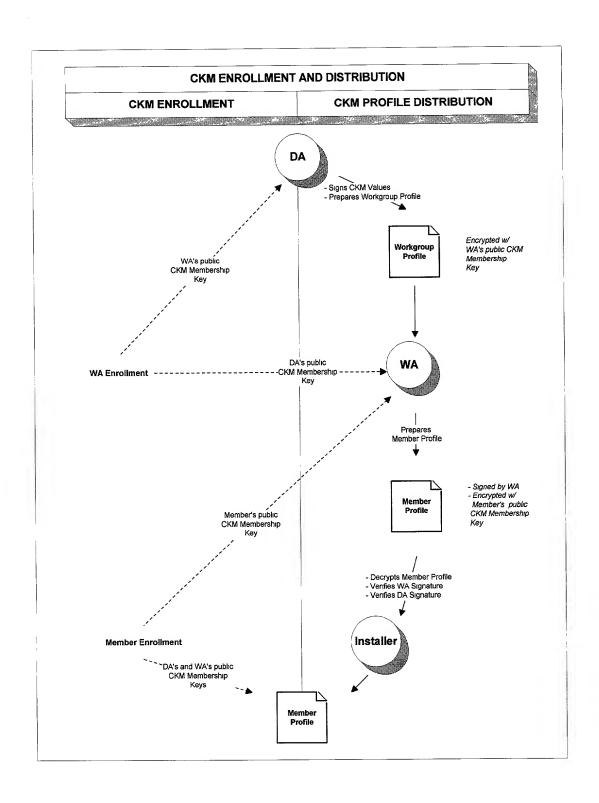


FIG. 16

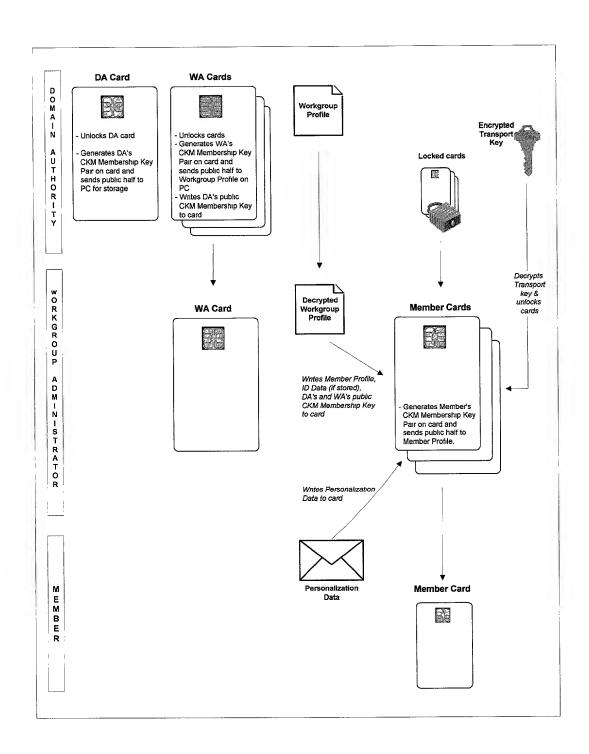


FIG. 17

FIG. 18

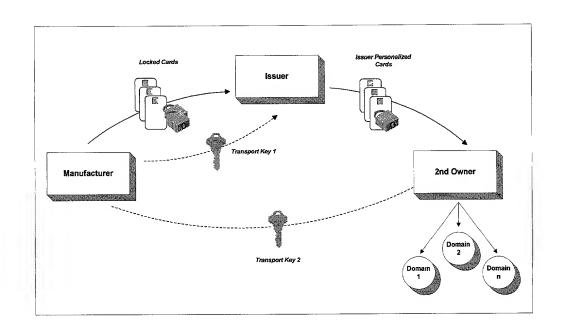


FIG. 19

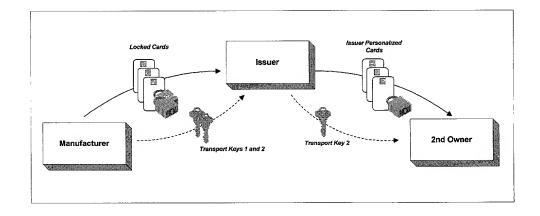
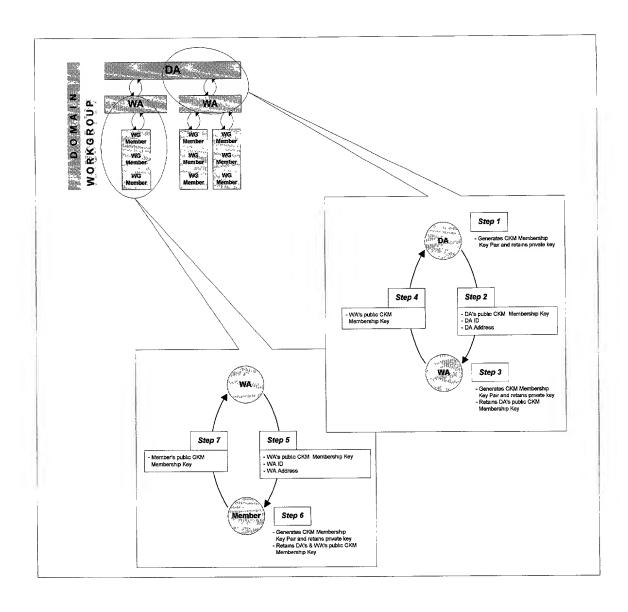
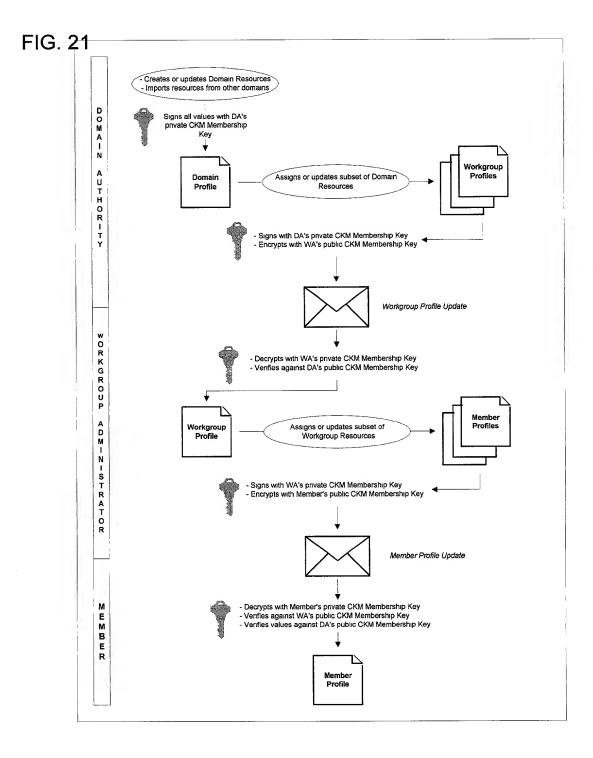


FIG. 20





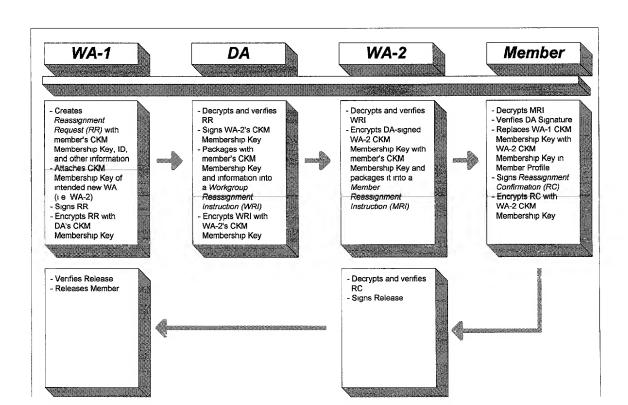
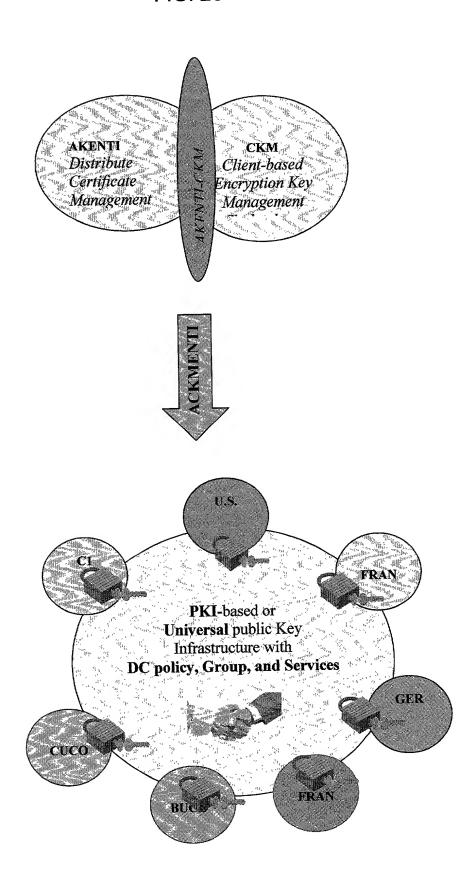


FIG. 23



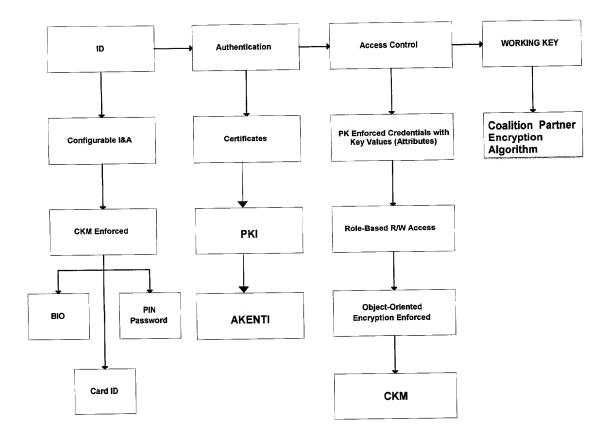


FIG. 24

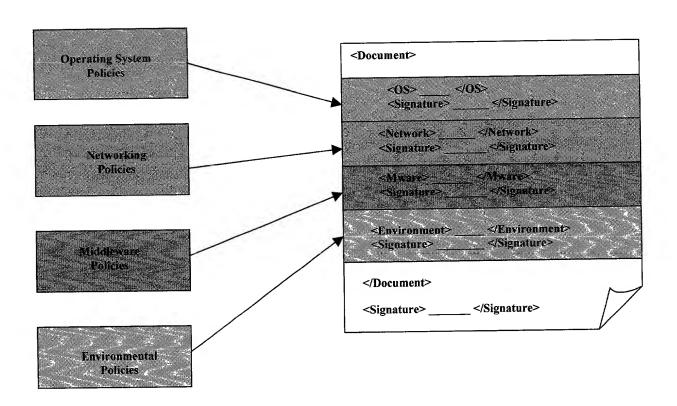
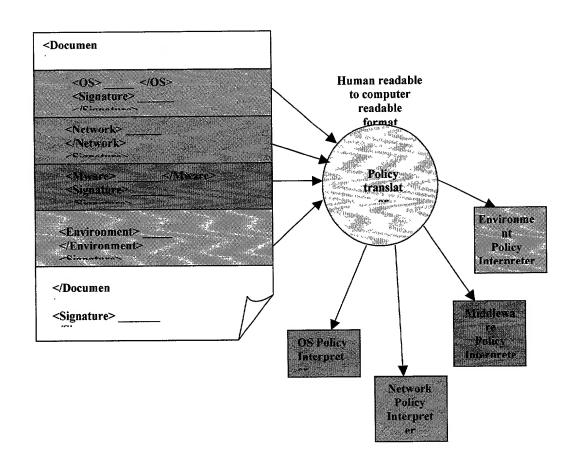
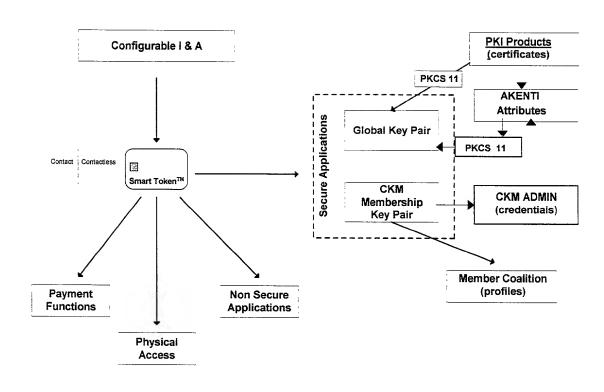


FIG. 25

FIG. 26





CKM TM I&A PK PKI

Constructive Key Management Identification and Authentication Public Key Public Key Infrastructure

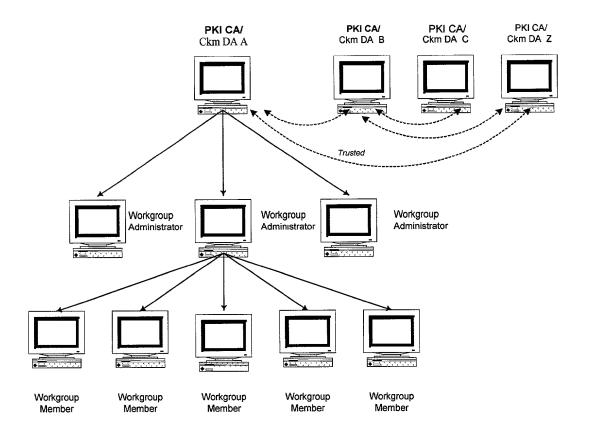


FIG. 28